information may include a name of the identified candidate. In some embodiments, the personal information may include a link to an online profile associated with the identified match. In some embodiments, the personal information transmitted to the user device is obtained from a webpage having the highest PageRank value among the webpages containing the personal information.

[0013] In some embodiments, the method also includes: (i) determining permission of access for the subject to a venue or an account based on the personal information of the identified candidate; (ii) granting the access for the subject if the identified candidate is an authorized user, or denying the access for the subject if the identified candidate is not an authorized user or a candidate matching the captured facial image cannot be identified; and (iii) transmitting a message indicative of granting or denying the access to the venue or the account. In some embodiments, the account is associated with a bank, a financial institute or a credit company.

[0014] In some embodiments, the method additionally includes providing access to the database to a plurality of users. The plurality users may be located in the same geographic area or associated with the same business type.

[0015] In some embodiments, the facial image data include a second captured facial image of a second subject. In some embodiments, the method includes identifying a relationship between two or more subjects having facial images captured in a single image.

[0016] In another aspect, this disclosure provides a method for verifying an identity of a user. The method includes: (a) providing a facial image data comprising a captured facial image and a personal identification number of the user; (b) transforming the facial image data to facial recognition data; (c) comparing the facial recognition data and the personal identification number to reference facial recognition data and reference personal identification numbers associated with a plurality of stored facial images of individuals to identify at least one likely candidate matching the captured facial image and the personal identification number; and (d) upon identification of the candidate, transmitting a confirmation to a user device indicating the user is an authorized user.

[0017] In another aspect, this disclosure also presents a system for providing information about a subject. The system includes: (i) a facial image processing module operable to transform a captured facial image of the subject to a facial recognition data; and (ii) a facial recognition module operable to: (a) compare the facial recognition data to reference facial recognition data associated with a plurality of stored facial images of individuals to identify at least one likely candidate matching the captured facial image, (b) upon identification of the candidate matching the captured facial image, retrieve from the database personal information associated with the candidate, and (c) transmit the personal information to the user device and cause the user device to display the personal information.

[0018] In some embodiments, the system includes a plurality of imaging devices, wherein each of the plurality of imaging devices is operable to capture at least one image comprising a face of the subject to generate a captured image. The plurality of imaging devices is wirelessly coupled to a monitoring station that stores the plurality of stored images.

[0019] In yet another aspect, this disclosure provides a method of providing security. The method includes (i) providing imaging devices in a plurality of areas through which individuals pass, wherein the imaging devices are operable to obtain facial images of each of the individuals; and (ii) performing facial recognition by the system as described above.

[0020] In some embodiments, the facial image processing module is operable to preprocess an image of the subject by the user device. Preprocessing may include detecting a facial image in the image of the subject by the user device. Preprocessing may also include cropping, resizing, gradation conversion, median filtering, histogram equalization, or size normalized image processing. In some embodiments, the facial image is captured by a camera-enabled user device. In some embodiments, the user device is provided in a customized enclosure with an opening for the camera. In some embodiments, the image is captured by a network camera. In some embodiments, the image is imported from a second user device. In some embodiments, the subject is a person. In some embodiments, the subject is a criminal. In some embodiments, the facial image data comprise a three-dimensional facial image of the subject.

[0021] In some embodiments, the facial image processing module is operable to: (i) download by a web crawler facial images of individuals and personal information associated therewith; and (ii) store the downloaded facial images and associated personal information in the database.

[0022] In some embodiments, the reference facial recognition data comprise the facial images downloaded by the web crawler. The reference facial recognition data may include the facial images obtained from the Internet, professional websites, law enforcement websites, or departments of motor vehicles. In some embodiments, the database comprises a plurality of criminal records associated with the facial images stored in the database.

[0023] In some embodiments, the facial recognition data include a vector representation of the captured facial image of the subject. Similarly, the reference facial recognition data may also include a vector representation of the stored facial image in the database. In some embodiments, the vector representation comprises a 512 point vector or a 1024×1024 facial data matrix.

[0024] In the system as described above, the facial recognition module is operable to compare the vector representation of the captured facial image of the subject to a vector representation associated with the stored facial images in the database. Comparing the facial recognition data can be performed by a machine learning module. The machine learning module comprises a deep convolutional neural network (CNN). In some embodiments, identification of the candidate is performed by the k-nearest neighbors algorithm (k-NN).

[0025] In some embodiments, the method may further include detecting a liveness gesture. The liveness gesture is based on at least one of a yaw angle of a second image relative to a first image and a pitch angle of the second image relative to the first image, wherein the yaw angle corresponds to a transition centered around a vertical axis, and wherein the pitch angle corresponds to a transition centered around a horizontal axis.

[0026] In some embodiments, the personal information is retrieved from the database based on a predetermined privacy setting of the identified candidate. In some embodiments, the method further includes displaying one or more facial images of the identified candidate and the personal